FINAL

Talking Points Prepared for Delivery by James B. Comey
Director, Federal Bureau of Investigation
American Law Institute Annual Meeting
Washington, D.C.
May 19, 2015

Introduction

- Good morning — great to be here with you
- I appreciate the good work ALI does to clarify and improve the law for all of us — whether we work in the courts, in government, the private sector, or academia
- I'm especially honored today to be introduced by Bill Webster, one of my predecessors as FBI Director
- It's also fitting, because your senior staff suggested I could talk about "challenges the Director and the FBI are facing that may be different today compared to the past"
- So I'd like to take a few minutes to do just that, and then I want to take your questions
- In many ways, the FBI today is much the same organization that Director Webster knew

- Full of dedicated, patriotic people, who do outstanding and often unsung work to keep our nation safe
- Still nobody better in the world at talking to people and finding out stuff — our fancy word for that these days is "intelligence" — in a lawful and appropriate way

- Still, a lot has changed for the FBI since Director Webster's time, and even since the last time I was in government at DOJ, in 2005

- Today I want to focus on one particular challenge that simply wasn't on our radar during Director Webster's tenure — cyber

Cyber

- One of the top priorities for my tenure as Director

- Cyber now touches every FBI program, and nearly every investigation

- We're in the midst of a transformation so fundamental that it's difficult to describe

- We've connected our entire lives to the Internet
  - It's where our children play, and where our money is
  - It's where we learn and shop and socialize

- It's where our secrets are — our health care, our critical infrastructure

- All the parts of life that the FBI is responsible for protecting — whether it's criminal, counterintelligence, counterterrorism, protecting children, fighting fraud — it all happens there

- I want to tell you how we're thinking about the cyber threat, and what our strategy is for addressing it

- [VECTOR]

- [JOHN DILLINGER ANALOGY]

The FBI's Response

- Before anything else, we must adopt an attitude of humility

- Arrogant and foolish to say, "I know what 10 years from now looks like, so the FBI should be deployed and equipped in this way"

- Must be humble enough to do things that seem reasonable, get feedback, and iterate

- Five-part strategy

- **One: Focus our resources**

- I view the cyber threat as a stack
- I've taken some ribbing for calling it an "evil layer cake," but I still like the analogy
  - State actors
  - Terrorists
  - Organized criminal groups
  - Hacktivists
  - Individual fraudsters
- FBI will focus our resources on the top layers of the stack, where we can have the greatest effect — high-level intrusions, state actors, global syndicates
- Second, we'll focus those resources in a different way
  - Cyber threat team model — assign the work not based on notions of physical jurisdiction or venue, but where the talent is

- **Two: Shrink the world**
  - The bad guys have shrunk the world to the size of a pin
  - We need to do the same thing

- We are going to forward-deploy more cyber Special Agents of the FBI and intelligence analysts around the world
    - Need to make sure that our battle rhythm keeps pace with the threat
- Within the government, we're going to continue to divide up our resources between organizations that handle cyber crime
    - Need to make sure that lanes in the road are clear
- When I left government in 2005, viewed our response to the threat as a bit like 4-year-old soccer
    - Clumps of children chasing the ball, because the ball is what's so cool
    - We all knew we had to do something about cyber, so there was a big clump of us running around chasing it
    - Now that I've come back, I see that we've made significant progress
    - More like high school – sometimes even college-level – soccer

        - We spread out, we know we have to pass, we know positioning is important
        - But we face a World Cup-level adversary
        - And so have to get better at feeding each other the ball and doing it at machine speed
        - Example: NCIJTF

- **Three: Impose costs**
    - Nation-states, international criminals, creeps down the street — they all think cyber is a freebie
    - First, we need to impose costs by laying hands on people and locking them up as often as possible
    - Second, we need to call out the conduct — say here's what happened and who did it
    - [Examples: Chinese/PLA hacker indictments, Sony/North Korea; Evgeniy Bogachev/GameOver Zeus botnet ; Encore Performance, Blackshades, Silk Road]
- **Four: Help state and local law enforcement partners deal with this threat**

- County sheriffs, local police departments, and local DAs are confronting all manner of cyber crimes that the FBI doesn't have the resources and time to handle
- We need to equip our state and local partners to be digitally literate
- For example, we're working with the Secret Service to offer cyber training to the 17,000 state and local law enforcement organizations in our country — much more needs to be done

- **Five: Improve relationships with our private sector partners**
  - Most of our infrastructure rests with our private partners – our technology, our innovation, our intellectual property
  - So, invariably, that's where the victims are
  - And that's where the information is that we need to respond to actions by nation states, terrorists, hacktivists — the entire layer cake manifests itself on private sector networks and systems
  - And if we can't find a way to share that information, we're sunk
  - It's a two-way street

- [50-FOOT WALL ANALOGY]
- I know some of the frustration on the private-sector side
- I was the general counsel of two companies before coming back to government
- And I've been in lots of conversations that went like this:
  - Why doesn't the government tell us what they know? What are they doing to do with what we tell them?
  - What if it gets used against us in the competitive marketplace? What if we get sued?
  - What will our shareholders think?
  - Why can't the government tell us things that we can actually do something about?
- We're getting better at this
  - Back in 2012, when financial institutions were being hit, one after the other, we provided classified briefings to private sector partners

- We disseminated intelligence reports to private sector partners with information about indicators of cyber crime
- We're doing this routinely now
- With this information, IT professionals can block particular IP addresses or respond appropriately if they find these indicators on their own systems

- But we still need to work past obstacles to sharing information
  - Legal — need clear rules of the road; Congress is working on this now
  - Technical
    - Need to be able to share information quickly, at machine speed
    - Example: Malware Investigator
  - Cultural [POST-SNOWDEN WIND]

Going Dark

- That brings me to another issue very much on my mind — what we call "Going Dark"
- I want to spend a few minutes on this, since it relates your current project on Principles of Data Privacy Law
- I've been talking about Going Dark a lot lately, because I was shocked by this when I came back to government
- When I left public service in 2005, this problem was blinking on my periphery
- When I came back in late 2013, it was blinking directly in front of me, because of
    - Proliferation of communication modes
    - Proliferation of encryption
- Those of us charged with protecting our citizens aren't always able to access the evidence we need to prosecute crime and prevent terrorism, even with lawful authority

- We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so

- We face two overlapping challenges
    - Data in motion
    - Data at rest
        - [BLACK COMPOSITION BOOK vs. THUMB DRIVE]

- Both types of data are increasingly encrypted

- It's the equivalent of a closet that can't be opened … a safe that can't be cracked — places that are **beyond the reach of the law**

- I'm deeply concerned about this, and I believe we got here because people fail to understand why law enforcement does what we do, and how we do it

- This is not just a national security issue; it also has serious implications for law enforcement's ability to protect **public safety**

- We need to be able to access communications and information to bring people to justice

- And we need to be able to do so quickly and efficiently — when time is of the essence

- Unfortunately, we are seeing more and more cases where we believe significant evidence resides on a phone or a laptop, but we can't crack the password

- We will continue to throw every lawful tool we have at this problem, but it's costly, inefficient, and it takes time

    - We usually don't have the benefit of time in our line of work

- I also know that our state and local partners don't have the resources, the personnel, or the technical specialists to handle these issues on an ad hoc basis

- We need a long-term fix, so we are all on the same page

    - So that communication providers know what is expected of them under the law

- So that we can do the jobs the American people have entrusted us to do, in the way they would want us to do them

- This is not about the government wanting to invade people's privacy

- I'm a big fan of privacy, and deeply skeptical of government power — I don't want the government, without lawful authority, going through anything of mine

- But I also don't think we, as a democracy, should just drift to a place where there are zones beyond the reach of the law in our country, even when we have court authority

- Maybe that's where we want to go, but to this point I don't think our country has talked enough yet about the trade-offs involved

- I hope that we can find a way to help the American public better understand the work of law enforcement, and the lawful means by which we do it

- Skepticism is good — but as a country, we don't want to drift to a place where we have to tell people, "I can't..."

- We need to find a way to balance privacy and skepticism about government with our need to protect innocent people

- We need to protect the **rule of law**, without creating areas that are **beyond the reach of the law**

Conclusion

- My thanks again to the American Law Institute, for all **your** work to protect the rule of law and to improve and interpret the law for new challenges

- Thank you for the chance to speak with you today

- Now I'm happy to take a few questions

###